

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



03 JAN 2005

(43) Internationales Veröffentlichungsdatum
15. Januar 2004 (15.01.2004)

PCT

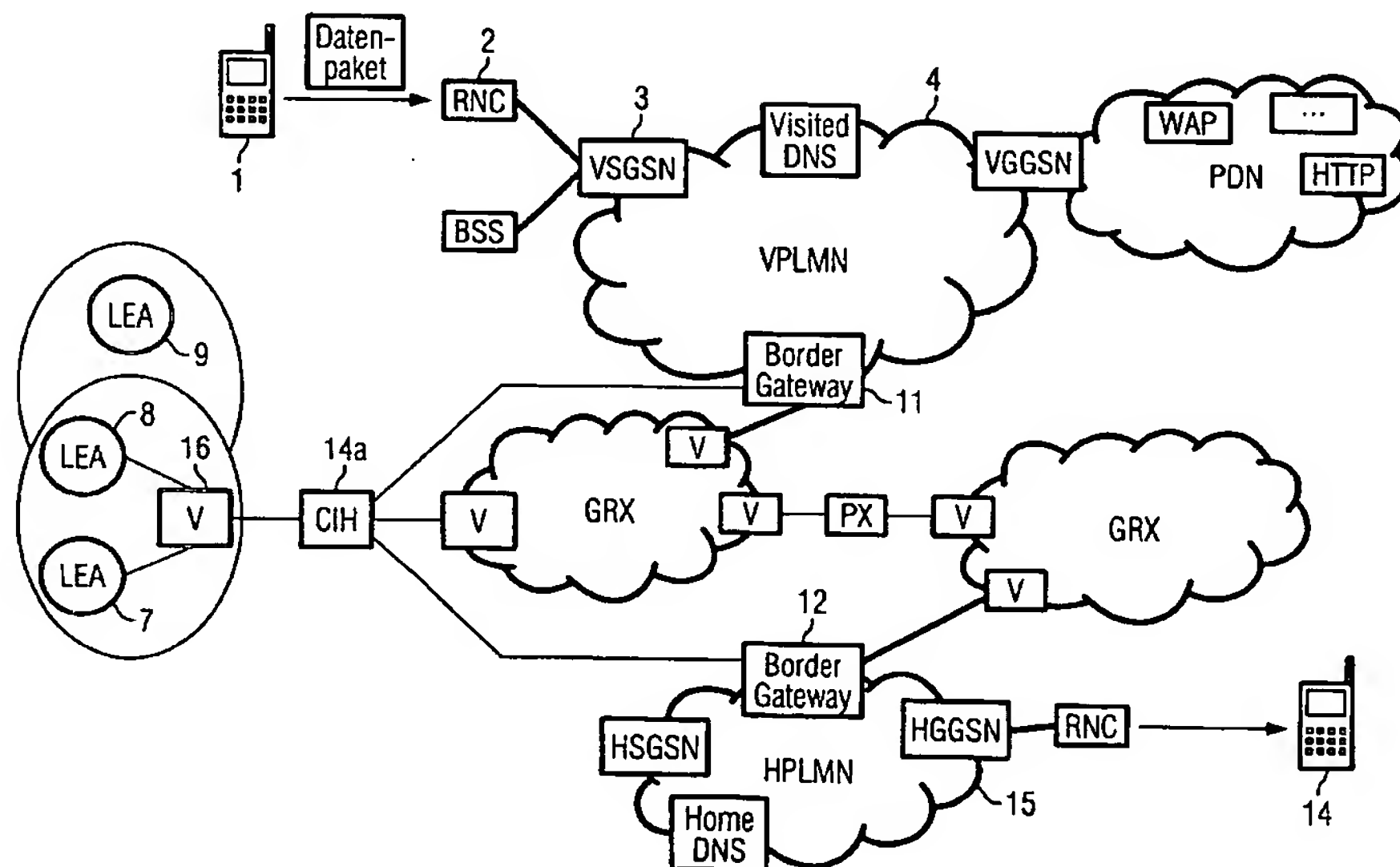
(10) Internationale Veröffentlichungsnummer
WO 2004/006553 A1

- (51) Internationale Patentklassifikation⁷: **H04M 3/22, H04L 12/26**
- (21) Internationales Aktenzeichen: **PCT/EP2002/007303**
- (22) Internationales Anmeldedatum:
2. Juli 2002 (02.07.2002)
- (25) Einreichungssprache: **Deutsch**
- (26) Veröffentlichungssprache: **Deutsch**
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): **SIEMENS AKTIENGESELLSCHAFT [DE/DE];** Wittelsbacherplatz 2, 80333 München (DE).
- (72) Erfinder; und
- (75) Erfinder/Anmelder (nur für US): **POLZER, Christian [AT/AT];** Spallartgasse 11/38, A-1140 Wien (AT). **PREGLER, Peter [AT/AT];** Mariahilfstr. 156-158 8/3/1, A-1150 Wien (AT). **SPALT, Bernhard [AT/AT];** Henrietenplatz 1/32, A-1150 Wien (AT).
- (74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT;** Postfach 22 16 34, 80506 München (DE).
- (81) Bestimmungsstaaten (national): **AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.**
- (84) Bestimmungsstaaten (regional): **ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).**

[Fortsetzung auf der nächsten Seite]

(54) Title: **CENTRAL EXCHANGE FOR AN IP MONITORING**

(54) Bezeichnung: **ZENTRALE VERMITTLUNGSSTELLE FÜR EINE IP-ÜBERWACHUNG**



DATENPAKET - DATA PACKET

(57) Abstract: An efficient and reliable monitoring of users of a telecommunication network is achieved by means of a method for the monitoring of a telecommunication user's data transmitted by a telecommunication network (4). Copies of the data are transmitted to at least one listening station (LEA 6;7;8;9), whereby the data is sent from an exchange device (VSGSN; HSGSN etc.), as a copy, to a monitoring handling device (CIH 14) and sent from said device (CIH 14) to one (7) of a number of addresses of listening stations (LEA 7;8;9) known thereto (CIH 14).

[Fortsetzung auf der nächsten Seite]

**Veröffentlicht:**

— mit internationalem Recherchenbericht

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Eine effiziente und zuverlässige Überwachung von Teilnehmern eines Telekommunikationsnetzes wird ermöglicht durch ein Verfahren zum Überwachen von über ein Telekommunikationsnetz (4) übertragenen Daten eines Telekommunikationsteilnehmers (1) durch Übertragung von Kopien der Daten an mindestens eine Abhörstelle (LEA 6;7;8;9) wobei die Daten von einer Vermittlungseinrichtung (VSGSN; HSGSN etc.) in Kopie an eine Überwachungsbehandlungseinrichtung (CIH 14) gesandt werden und von dieser (CIH 14) an jeweils eine (7) von mehreren ihr (CIH 14) bekannten Adressen von Abhörstellen (LEA 7;8;9) gesandt werden.

Beschreibung

"Zentrale Vermittlungsstelle für eine IP- Überwachung"

- 5 Die Erfindung betrifft Verfahren und Vorrichtungen zum Ermöglichen der Überwachung von über ein Mobilfunknetz übertragenen Daten.

10 Eine dem Fachmann bekannte Überwachung von Gesprächen zwischen Mobilfunkteilnehmern gemäß Figur 1 sieht vor, dass die Kommunikation (Gespräche oder Multimediatatenübertragung) zwischen zwei Mobilfunkteilnehmern eines oder mehrerer Mobilfunknetze überwacht wird, indem die zwischen den Mobilfunkteilnehmern übertragenen Nutzdaten auf ihrem Weg
15 durch (mindestens) ein Mobilfunknetz in einer Vermittlungseinrichtung (beispielsweise SGSN), welche eine Liste mit Identitäten abzuhörender Teilnehmer (MSISDN und/oder IMSI und/oder IMEI) gespeichert hat, kopiert werden und die kopierten Nutzdaten über eine Schnittstelle (= Boarder Gateway) an Überwachungseinrichtungen der
20 Geheimdienste/Bundesgrenzschutz /Polizei etc. übermittelt werden. Da es mehrere Behörden in mehreren örtlichen Niederlassungen gibt, die für die Überwachung von Mobilfunkteilnehmern zuständig sein können, werden die
25 kopierten Daten von Vermittlungseinrichtungen, welche die Daten zum Abhören kopieren, an weitere Vermittlungseinrichtungen (Boarder Gateways) an Netzübergängen des Mobilfunknetzes übermittelt, welche zu jeweils einer der Abhörstellen LEA (der Polizei oder des
30 Bundesgrenzschutzes etc.) eine sichere Verbindung wie beispielsweise einen IP-sec-Tunnel über das Internet etc. aufbauen, über welchen verschlüsselt die Daten an die zuständige Abhörstelle übermittelt werden. Da die Übertragung an die Abhörstellen LEA ausführende Vermittlungsstellen an
35 Grenzen eines Mobilfunknetzes zumindest einmal pro Mobilfunknetz vorzusehen sind und die Übertragung zu jeder Abhörstelle LEA getrennt erfolgt, ist eine

Schlüsselverwaltung (Key Management) in jeder dieser Schnittstellen-Vermittlungseinrichtungen (Boarder Gateway) für jede der Abhörstellen erforderlich.

- 5 Aufgabe der vorliegenden Erfindung ist es, die Überwachung abzuhörender Daten von Teilnehmern eines Mobilfunknetzes effizient und zuverlässig zu ermöglichen. Die Aufgabe wird jeweils durch die Gegenstände der unabhängigen Ansprüche gelöst.

10

- Durch die erfindungsgemäße Überwachungsbehandlungseinrichtung (= Central Interception Handler CIH), über welche abzuhörende Daten an Abhörstellen der unterschiedlichen zuständigen Behörden übertragen werden, wird die Schlüsselverwaltung (Key Management) verglichen mit der bisher praktizierten Lösung der Einzelverbindungen von Abhörstellen LEA zu Schnittstellenvermittlungseinrichtungen (Boarder Gateway) erheblich vereinfacht. Dennoch bleibt die Übertragung der abgehörten Daten zu den Abhöreinrichtungen sehr sicher und ist beispielsweise auch über das Internet möglich, da (erfindungsgemäß in einfach administrierbarer Weise) eine verschlüsselte Übertragung von der Überwachungsbehandlungseinrichtung CIH zu den Abhörstellen LEA erfolgen kann. Dabei kann beispielsweise pro Mobilfunknetz oder von mehreren Mobilfunknetzen nur eine Überwachungsbehandlungseinrichtung CIH verwendet werden oder es können für ein Mobilfunknetz mehrere Überwachungsbehandlungseinrichtungen verwendet werden.

- 25 30 Weitere Merkmale und Vorteile geben sich aus den Ansprüchen und der nachfolgenden Beschreibung eines Ausführungsbeispiels anhand der Zeichnung. Dabei zeigt:

- Figur 1 als Blockschaltbild eine Überwachung von über ein Mobilfunknetz übertragenen Nutzdaten gemäß dem Stand der Technik mit Einzelverbindungen zwischen Vermittlungseinrichtungen (Boarder Gateways) und

35

Abhörstellen (LEA) seitens jeweils zuständiger Behörden,

Figur 2 als Blockschaltbild die erfindungsgemäße Überwachung von über ein Mobilfunknetz übertragenen Daten mit einer zentralen Überwachungsbehandlungseinrichtung CIH.

Figur 1 zeigt als Blockschaltbild ein Mobilfunkendgerät 1 (eine Mobilstation, einen Communicator etc.), welche über eine Luftschnittstellenübertragungseinrichtung (RNC oder BS) 2 und über eine Vermittlungseinrichtung (VSGSN etc.) 3 eines ersten Mobilfunknetzes 4 und ggf. ein weiteres Mobilfunknetz oder ein Festnetz mit einem weiteren Teilnehmer (14) kommuniziert oder über einen Internetzugang über das Internet (http / wap etc.) kommuniziert. Im in der Figur 1 dargestellten Beispiel wird den jeweils zuständigen Behörden (Polizei/Bundesgrenzschutz/Geheimdienst usw.) mit jeweils einer Abhörstelle LEA 6,7,8,9 ermöglicht, Gespräche von Teilnehmern 1 über ein Mobilfunknetz 4 zu überwachen, indem das Gespräch (oder die Multimediadatenübertragung über das Internet etc.) repräsentierende Daten auf ihrem Weg durch das Mobilfunknetz 4 von einer Vermittlungseinrichtung (SGSN oder VSGSN oder HSGSN oder sonstige Vermittlungsstelle V) 3 (soweit sie von gemäß einer in der Vermittlungsstelle 3 vorhandenen Liste als von zu überwachenden Geräten oder Personen (1) stammen), identifiziert werden (beim Einbuchen oder durch Überwachung des Datenstromes), und in Kopie an eine Schnittstellenvermittlungseinrichtung (Boarder Gateway) 11 übertragen werden, welche die kopierten Daten zu der für die Überwachung dieses Teilnehmers(1) oder seines Endgerätes zuständigen Abhörstelle (Abhöreinrichtungen mit Computern oder Aufnahmeeinrichtungen oder Telefon etc.) der zuständigen Behörde in einem gesicherten Tunnel, beispielsweise IP-sec-Tunnel überträgt. Hierfür ist in jedem Mobilfunknetz mindestens eine Schnittstellenvermittlungseinrichtung (Boarder Gateway) 11,12 vorgesehen, welche zu jeder der

Abhörstellen 6 bis 9 jeweils eine eigene Verbindung aufbaut. Da die Übertragung zwischen den Schnittstellenvermittlungseinrichtungen (Boarder Gateway) 11, 12 und den Abhörstellen 7 bis 9 möglichst abhörsicher erfolgen soll, erfolgt sie beispielsweise verschlüsselt, wobei für die Übertragung zu verwendete Schlüssel in jeder Vermittlungseinrichtung 11,12 für jede Abhörstelle 6 bis 9 eigens verwaltet werden müssen (Key Management).

5

10 Gemäß Figur 2 wird die Überwachung von über ein Mobilfunknetz übertragenen Daten durch eine Überwachungsbehandlungseinrichtung CIH 14 unterstützt, welche die Schlüsselverwaltung für die gesicherte (verschlüsselte) Übertragung über ein paketvermittelltes Netz (beispielsweise

15 per Ipsec) erheblich vereinfacht. Wie schon zu Figur 1 erläutert werden auch im Beispiel in Figur 2 Daten (Sprachdaten oder andere Nutzdaten), eines Mobilfunkteilnehmers über ein Mobilfunknetz (oder ein anderes Telekommunikationsnetz) paketvermittelt an ein weiteres

20 Telekommunikationsnetz (Mobilfunknetz, oder Festnetz, oder Internet, oder anderes paketvermittelltes Netz) übertragen. Auf ihrem Weg durch das Telekommunikationsnetz 4 werden die Daten (Datenpakete) von einer Vermittlungseinrichtung (welche eine Tabelle zu überwachende Teilnehmer gespeichert hat) kopiert

25 und die Kopien der Daten über eine Vermittlungseinrichtung (Boarder Gateway) an Abhörstellen LEA übertragen. Dabei wird jedoch erfindungsgemäß nicht ein Tunnel zwischen den Schnittstellenvermittlungseinrichtungen (Boarder Gateways 11,12) und den Abhörstellen 6,7,8,9 aufgebaut, sondern

30 zwischen der Schnittstellenvermittlungseinrichtung 11 (oder 12) und einer zentralen Überwachungsbehandlungseinrichtung CIH 14, welche eine sichere Übertragung (beispielsweise per Internetprotokoll oder in einem anderen paketvermittelten Protokoll über das Internet oder ein anderes Netz) zu der

35 zuständigen Abhörstelle 7 für diesen Teilnehmer durchführt. Hierfür hat die Überwachungseinrichtung 14 eine Tabelle von Adressen (IP-Adressen) aller Abhörstellen LEA 6,7,8,9.

Überdies besitzt die Überwachungsbehandlungseinrichtung CIH 14 einen Speicher (oder Zugriff auf einen Speicher) mit einer Liste von Schlüsseln, wobei für jeweils eine bestimmte Abhörstelle LEA 6/7/8/9 jeweils mindestens ein Schlüssel
5 abgelegt ist, mit welchem verschlüsselt die abgehörten Daten zu dieser Abhörstelle 6/7/8/9 zu übertragen sind. Im dargestellten Beispiel werden die Daten von der Überwachungsbehandlungseinrichtung 14 an die jeweils zuständige (mindestens eine) Abhörstelle 6,7,8,9 für alle
10 Abhörstellen über die gleiche paketvermittelte Vermittlungseinrichtung (Router V) 16 übertragen.

Vorteilhafterweise muss erfindungsgemäß die Adresse (IP-Adresse etc.) der zuständigen Abhörstelle LEA 6/7/8/9 nur der
15 Überwachungseinrichtung CIH 14 bekannt sein und nicht jeder Schnittstellenvermittlungseinrichtung (Boarder Gateway) 11,12 und auch die Schlüsselverwaltung muss nur in der Überwachungsbehandlungseinrichtung 14 (Central Interception Handler CIH) erfolgen.

20 Durch eine Liste der Zuordnungen im CIH sind erforderliche Adressumsetzungen möglich.

25 Die Übertragung der Daten zwischen den Schnittstellenvermittlungseinrichtungen (Boarder Gateway) 11, 12 eines Netzes, erfolgt beispielsweise über eine gesicherte Verbindung / Ipsec- Tunnel zwischen Vermittlungseinrichtungen Boarder Gateway und der Überwachungsbehandlungseinrichtung 14
30 übertragen. Die Überwachungsbehandlungseinrichtung CIH 14 kann Teil des Netzwerks sein, in welchem eine oder alle Abhörstellen 6 bis 9 angeordnet sind, also sich in diesem Netzwerk befinden.

Patentansprüche

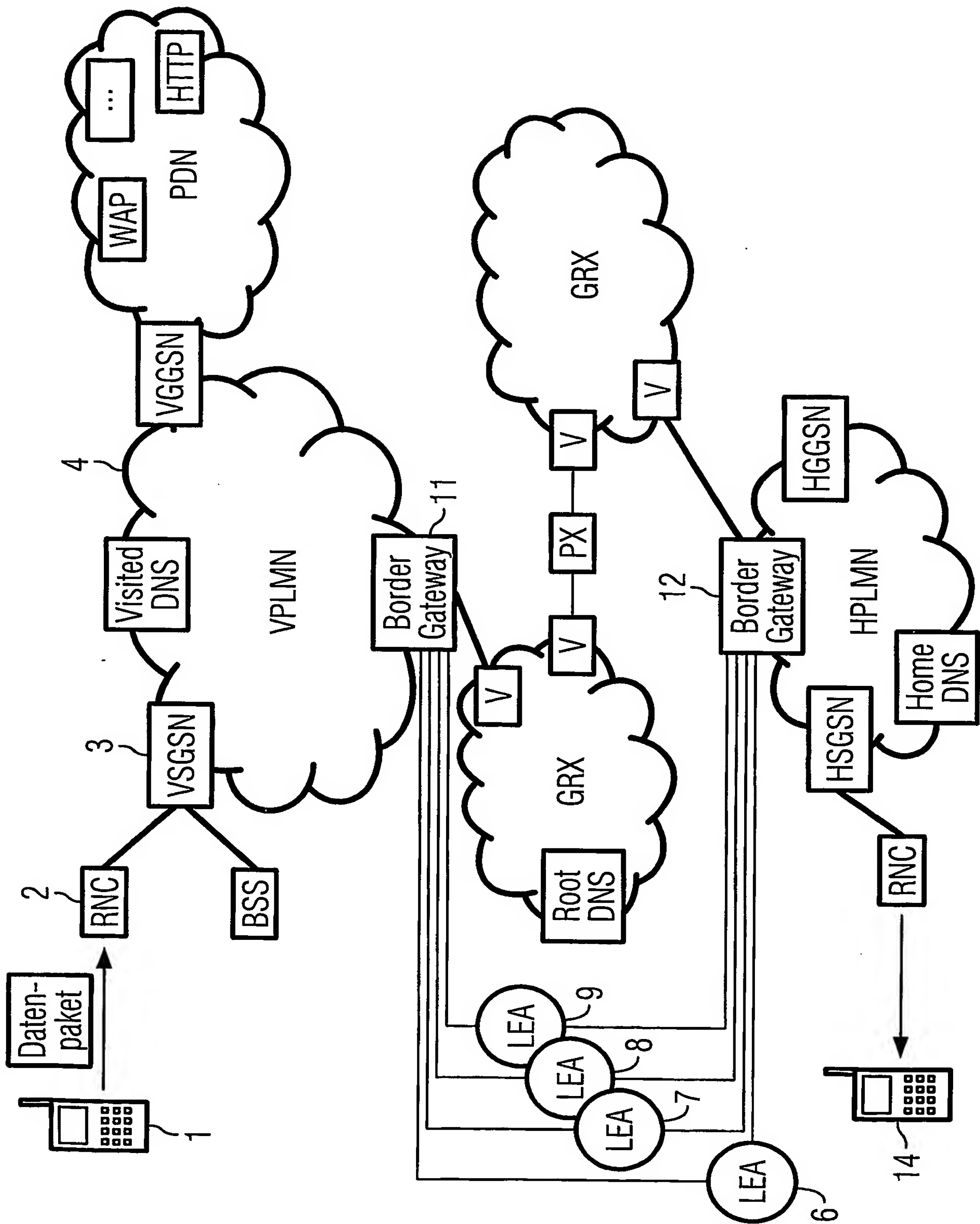
1. Verfahren zum Ermöglichen der Überwachung von über ein
Telekommunikationsnetz (4) übertragenen Daten eines
5 Telekommunikationsteilnehmers (1) durch Übertragung von
Kopien der Daten an mindestens eine Abhörstelle (LEA
6;7;8;9),
d a d u r c h g e k e n n z e i c h n e t,
dass die Daten von einer Vermittlungseinrichtung (VSGSN;
10 HSGSN etc.) in Kopie an eine
Überwachungsbehandlungseinrichtung (CIH 14) gesandt
werden und von dieser (CIH 14) an jeweils eine (7) von
mehreren ihr (CIH 14) bekannten Adressen von
Abhörstellen (LEA 6;7;8;9) gesandt werden.
15
2. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t,
dass nur die Überwachungsbehandlungseinrichtung (CIH 14)
die Adresse (LEA-IP-Adresse von 6;7;8;9) der
20 Abhörstellen (LEA 6;7;8;9) kennt, insbesondere in einer
Tabelle in einem Speicher gespeichert hat.
3. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t,
25 dass das Telekommunikationsnetz ein Mobilfunknetz ist.
4. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t,
dass das Telekommunikationsnetz ein paketvermitteltes
30 Netz, insbesondere IP-Protokoll-Netz ist.
5. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t,
dass die Vermittlungseinrichtungen (VSGSN 3; HSGSN...)
35 die abzuhörenden kopierten Daten an eine
Schnittstellenvermittlungseinrichtung (Boarder Gateway
11;12) senden, welche die Adresse der

Überwachungsbehandlungseinrichtung (CIH 14) kennen, insbesondere in einem Speicher gespeichert haben.

- 5 6. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t, .
dass die Abhörstellen (LEA 6;7;8;9) verschiedene
Adressen haben (LEA-IP-Adresse), die die
Überwachungsbehandlungseinrichtung (CIH) kennt.
- 10 7. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t,
dass die Überwachungsbehandlungseinrichtung (14) sich im
gleichen Netzwerk befindet wie die Abhörstellen (7 bis
9) .
- 15 8. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t,
dass ein Sicherheitstunnel, insbesondere IP-sec-Tunnel,
zwischen der Überwachungsbehandlungseinrichtung (14) und
20 den Schnittstellenvermittlungseinrichtungen (Boarder
Gateway 11,12) aufgebaut ist oder für eine Überwachung
eines Gesprächs aufgebaut wird.
- 25 9. Verfahren nach einem der vorhergehenden Ansprüche
d a d u r c h g e k e n n z e i c h n e t,
dass mehrere Überwachungsbehandlungseinrichtungen (CIH
11; 12) in einem Mobilfunknetz (4) angeordnet sind.
- 30 9. Verfahren nach einem der Ansprüche 1 bis 8
d a d u r c h g e k e n n z e i c h n e t,
dass in einem Mobilfunknetz jeweils nur eine
Überwachungseinrichtung (11;12) angeordnet ist.
- 35 11. Vorrichtung (CIH 14), insbesondere zur Durchführung des
Verfahrens nach einem vorhergehenden Ansprüche,

mit einer Schnittstelle zu mindestens einer
Vermittlungseinrichtung (Boarder Gateway 11,12), für den
Empfang von abzuhörenden Daten,
mit einem Speicher mit einer Liste von Adressen und
5 Schlüsseln von mehreren Abhörstellen (6;7;8;9),
mit einer Schnittstelle zum Übertragen von über die
erste Schnittstelle von einer Vermittlungseinrichtung
(11) empfangenen abzuhörenden Daten eines Endgerätes (1)
an eine aufgrund der Identität des Teilnehmers
10 (MSISDN, ISDN, MEI etc.) und der in einem Speicher in der
Vorrichtung (14) gespeicherten Liste identifizierten IP-
Adresse einer Abhörstelle (6;7;8;9).

FIG 1



INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/07303

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04M3/22 H04L12/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04M H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/078384 A1 (HIPPELAINEN LASSI) 20 June 2002 (2002-06-20) abstract; figures 1-4 page 1, paragraphs 1-20 page 2, paragraph 29 page 3, paragraph 52 -page 4, paragraph 71 ---	11
X	WO 01 91374 A (BJOERNSSON STEFAN ;ERICSSON TELEFON AB L M (SE); LINDBERG NICLAS ()) 29 November 2001 (2001-11-29) abstract page 3, line 1 -page 4, line 14 page 5, line 23-30 page 7, line 20,21 page 13, line 1 -page 24, line 30 ---	1,2,5-7, 11
A	abstract page 3, line 1 -page 4, line 14 page 5, line 23-30 page 7, line 20,21 page 13, line 1 -page 24, line 30 ---	3,4,8-10
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

20 February 2003

Date of mailing of the international search report

07/03/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Tillgren, M

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 02/07303

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 02 49329 A (HALBRAICH ERAN ;ILAN TOMER (IL); YOSEF ILAN (IL); NICE SYSTEMS LTD) 20 June 2002 (2002-06-20) the whole document	1-11
A	US 2002/075880 A1 (DOLINAR LARRY ET AL) 20 June 2002 (2002-06-20) the whole document	1-11
A	US 5 627 819 A (DEV ROGER ET AL) 6 May 1997 (1997-05-06) the whole document	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP02/07303

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2002078384	A1	20-06-2002	WO 0042742 A1 AU 2617399 A EP 1142218 A1 JP 2002535883 T	20-07-2000 01-08-2000 10-10-2001 22-10-2002
WO 0191374	A	29-11-2001	AU 6092601 A WO 0191374 A1	03-12-2001 29-11-2001
WO 0249329	A	20-06-2002	AU 2247902 A WO 0249329 A2	24-06-2002 20-06-2002
US 2002075880	A1	20-06-2002	NONE	
US 5627819	A	06-05-1997	AT 190787 T AU 686048 B2 AU 4856796 A DE 69607142 D1 DE 69607142 T2 EP 0803157 A2 JP 10512413 T WO 9621982 A2 US 5754532 A	15-04-2000 29-01-1998 31-07-1996 20-04-2000 28-09-2000 29-10-1997 24-11-1998 18-07-1996 19-05-1998

INTERNATIONALER RECHERCHENBERICHT

Intern. Aktenzeichen

PCT/EP 02/07303

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04M3/22 H04L12/26

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04M H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2002/078384 A1 (HIPPELAINEN LASSI) 20. Juni 2002 (2002-06-20) Zusammenfassung; Abbildungen 1-4 Seite 1, Absätze 1-20 Seite 2, Absatz 29 Seite 3, Absatz 52 -Seite 4, Absatz 71 ---	11
X	WO 01 91374 A (BJOERNSSON STEFAN ;ERICSSON TELEFON AB L M (SE); LINDBERG NICLAS ()) 29. November 2001 (2001-11-29) Zusammenfassung Seite 3, Zeile 1 -Seite 4, Zeile 14 Seite 5, Zeile 23-30 Seite 7, Zeile 20,21 Seite 13, Zeile 1 -Seite 24, Zeile 30 ---	1,2,5-7, 11
A		3,4,8-10
	-/--	

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche

20. Februar 2003

Absenddatum des internationalen Recherchenberichts

07/03/2003

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Tillgren, M

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 02 49329 A (HALBRAICH ERAN ;ILAN TOMER (IL); YOSEF ILAN (IL); NICE SYSTEMS LTD) 20. Juni 2002 (2002-06-20) das ganze Dokument ---	1-11
A	US 2002/075880 A1 (DOLINAR LARRY ET AL) 20. Juni 2002 (2002-06-20) das ganze Dokument ---	1-11
A	US 5 627 819 A (DEV ROGER ET AL) 6. Mai 1997 (1997-05-06) das ganze Dokument -----	1-11

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die derselben Patentfamilie gehören

Internationaler Aktenzeichen

PCT/EP 02/07303

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 2002078384	A1	20-06-2002	WO	0042742 A1	20-07-2000
			AU	2617399 A	01-08-2000
			EP	1142218 A1	10-10-2001
			JP	2002535883 T	22-10-2002

WO 0191374	A	29-11-2001	AU	6092601 A	03-12-2001
			WO	0191374 A1	29-11-2001

WO 0249329	A	20-06-2002	AU	2247902 A	24-06-2002
			WO	0249329 A2	20-06-2002

US 2002075880	A1	20-06-2002	KEINE		

US 5627819	A	06-05-1997	AT	190787 T	15-04-2000
			AU	686048 B2	29-01-1998
			AU	4856796 A	31-07-1996
			DE	69607142 D1	20-04-2000
			DE	69607142 T2	28-09-2000
			EP	0803157 A2	29-10-1997
			JP	10512413 T	24-11-1998
			WO	9621982 A2	18-07-1996
			US	5754532 A	19-05-1998

DT05 Rec'd PCT/PTO 03 JAN 2005

Description

"Central exchange for IP monitoring"

- 5 The invention relates to methods and devices for enabling data transmitted over a public land mobile network to be monitored.

A means of monitoring calls between mobile radio users that is known to the person skilled in the art, as illustrated in
10 Figure 1, provides that the communication (conversations or multimedia data transmission) between two mobile radio users of one or more public land mobile networks is monitored in that the user data transmitted between the mobile radio users, while on its way through (at least) one public land mobile network,
15 is copied in a switching device (for example SGSN) which has stored a list containing identities of users subject to call-tapping (MSISDN and/or IMSI and/or IMEI) and the copied user data is transmitted via an interface (= border gateway) to monitoring devices belonging to the secret intelligence
20 services, federal border police, police, etc. Since there are a number of government agencies in a number of local offices that can be responsible for monitoring mobile radio users, the copied data is transmitted by switching devices which copy the data to be intercepted to further switching devices (border
25 gateways) at network gateways of the public land mobile network, which gateways each set up a secure connection, such as, for example, an IPsec tunnel over the Internet etc., to one of the listening stations LEA (of the police or the federal border police, etc.), via which secure connection the data is
30 transmitted in encrypted form to the listening station responsible. As the exchanges carrying out the transmission to the listening stations LEA at borders of a public land mobile network are to be provided at least once per public land mobile network and the transmission is performed separately to each

listening station LEA, a key management means is required in each of these interface switching devices (border gateways) for each of the listening stations.

5 The object of the present invention is to enable the monitoring of data to be intercepted which is associated with users of a public land mobile network in an efficient and reliable manner. This object is achieved in each case by the subject matter of the independent claims.

10

The inventive monitoring handling device (= Central Interception Handler CIH) via which data to be intercepted is transmitted to listening stations of the different government agencies responsible considerably simplifies key management compared with the previously practised solution of individual connections from listening stations LEA to interface switching devices (border gateways). Nevertheless the transmission of the intercepted data to the listening devices is still very secure and is also possible for example via the Internet, since (in an easy-to-administer manner according to the invention) an encrypted transmission can take place from the monitoring handling device CIH to the listening stations LEA. At the same time it is possible for only one monitoring handling device CIH to be used per public land mobile network or by a number of public land mobile networks, for example, or alternatively a plurality of monitoring handling devices can be used for one public land mobile network.

Further features and advantages will emerge from the claims and the following description of an exemplary embodiment with reference to the drawing, in which:

Figure 1 is a block diagram showing the monitoring of user data transmitted over a public land mobile network

according to the prior art having individual connections between switching devices (border gateways) and listening stations (LEA) on the side of competent government agencies in each case,

5 Figure 2 is a block diagram showing the monitoring of data transmitted over a public land mobile network according to the invention having a central monitoring handling device CIH.

10 Figure 1 is a block diagram showing a mobile radio terminal device 1 (a mobile station, a communicator etc.) which communicates with a further user (14) via an air interface transmission device (RNC or BS) 2 and via a switching device (VSGSN etc.) 3 of a first public land mobile network 4 and
15 possibly a further public land mobile network or a fixed network or via an Internet access point over the Internet (http / wap etc.). In the example shown in Figure 1 it is made possible for the competent government agencies in each case (police/federal border police/secret intelligence service
20 etc.), each having a listening station LEA 6, 7, 8, 9, to monitor calls of users 1 over a public land mobile network 4 in such a way that data representing the call (or the multimedia transmission over the Internet, etc.) is identified (during registration or by monitoring of the data stream) on its way
25 through the public land mobile network 4 by a switching device (SGSN or VSGSN or HSGSN or other exchange V) 3 (insofar as said data originates from devices or persons (1) to be monitored according to a list held in the exchange 3) and a copy of said data is transmitted to an interface switching device (border
30 gateway) 11 which in turn transmits the copied data in a secure tunnel, for example an IPsec tunnel, to the competent government agency's listening station (bugging devices with computers or recording devices or telephone etc.) responsible for monitoring said user (1) or his terminal device. For this

purpose there is provided in each public land mobile network at least one interface switching device (border gateway) 11, 12 which sets up a separate connection in each case to each of the listening stations 6 to 9.

5 As the transmission between the interface switching devices (border gateways) 11, 12 and the listening stations 7 to 9 is ideally to be executed in an intercept-proof manner, it takes place for example in encrypted form, with keys to be used for the transmission having to be administered separately in each
10 switching device 11, 12 for each listening station 6 to 9 (key management).

According to Figure 2 the monitoring of data transmitted over a public land mobile network is supported by a monitoring
15 handling device CIH 14 which considerably simplifies the key management for the secure (encrypted) transmission over a packet-switched network (for example by means of IPsec). As already explained in relation to Figure 1, in the example shown in Figure 2 data (voice data or other user data) of a mobile
20 radio user is also transmitted over a public land mobile network (or some other telecommunication network) by means of packet switching to a further telecommunication network (public land mobile network, or fixed network, or Internet, or other packet-switched network). On its way through the
25 telecommunication network 4 the data (data packets) is copied by a switching device (which has stored a table of users to be monitored) and the copies of the data are transmitted via a switching device (border gateway) to listening stations LEA. In the process, however, according to the invention a tunnel will
30 be set up, not between the interface switching devices (border gateways 11, 12) and the listening stations 6, 7, 8, 9, but between the interface switching device 11 (or 12) and a central monitoring handling device CIH 14 which performs a secure transmission (for example using the Internet Protocol or in

some other packet-switched protocol over the Internet or another network) to the listening station 7 responsible for this user. For this purpose the monitoring device 14 has a table of addresses (IP addresses) of all the listening stations
5 LEA 6, 7, 8, 9.

In addition the monitoring handling device CIH 14 has a memory (or access to a memory) containing a list of keys, with at least one key being stored for a specific listening station LEA
10 6/7/8/9 in each case, by means of which key the intercepted data is to be transmitted to this listening station 6/7/8/9 in encrypted form. In the example shown, the data is transmitted by the monitoring handling device 14 to the respective competent (at least one) listening station 6, 7, 8, 9 for all
15 listening stations via the same packet-switched switching device (router V) 16.

Advantageously according to the invention the address (IP address etc.) of the competent listening station LEA 6/7/8/9
20 must be known only to the monitoring device CIH 14 and not to each interface switching device (border gateway) 11, 12 and the key management also only has to take place in the monitoring handling device 14 (Central Interception Handler CIH).

25 Necessary address translations are possible based on a list of the assignments in the CIH.

The transmission of the data between the interface switching devices (border gateways) 11, 12 of a network takes place for
30 example over a secure connection/IPsec tunnel between switching devices (border gateways) and the monitoring handling device 14. The monitoring handling device CIH 14 can be part of the network in which one or all of the listening stations 6 to 9 are disposed, in other words can be located in this network.

Claims

1. A method for enabling the monitoring of data associated with a telecommunication user (1), said data being transmitted
5 over a telecommunication network (4), by transmission of copies of the data to at least one listening station (LEA 6; 7; 8; 9),
c h a r a c t e r i z e d i n t h a t
a copy of the data is sent by a switching device (VSGSN; HSGSN etc.) to a monitoring handling device (CIH 14) and is
10 in turn sent by the latter (CIH 14) to one (7) of a number of addresses of listening stations (LEA 6; 7; 8; 9) known to it (CIH 14) in each case.
- 15 2. The method according to one of the preceding claims [sic],
c h a r a c t e r i z e d i n t h a t
only the monitoring handling device (CIH 14) knows the addresses (LEA IP address of 6; 7; 8; 9) of the listening stations (LEA 6; 7; 8; 9), and in particular has stored said
20 addresses in a table.
3. The method according to one of the preceding claims,
c h a r a c t e r i z e d i n t h a t
the telecommunication network is a public land mobile
25 network.
4. The method according to one of the preceding claims,
c h a r a c t e r i z e d i n t h a t
the telecommunication network is a packet-switched network,
30 in particular an IP protocol network.
5. The method according to one of the preceding claims,
c h a r a c t e r i z e d i n t h a t

the switching devices (VSGSN 3; HSGSN...) send the copies of the data to be intercepted to an interface switching device (border gateway 11; 12) which knows the address of the monitoring handling device (CIH 14), and in particular has
5 stored said address in a memory.

6. The method according to one of the preceding claims,
c h a r a c t e r i z e d i n t h a t
the listening stations (LEA 6; 7; 8; 9) have different
10 addresses (LEA IP address) which are known to the monitoring
handling device (CIH).

7. The method according to one of the preceding claims,
c h a r a c t e r i z e d i n t h a t
15 the monitoring handling device (14) is located in the same
network as the listening stations (7 to 9).

8. The method according to one of the preceding claims,
c h a r a c t e r i z e d i n t h a t
20 a security tunnel, in particular an IPsec tunnel, is set up
between the monitoring handling device (14) and the
interface switching devices (border gateway 11, 12) or will
be set up for the purpose of monitoring a call.

25 9. The method according to one of the preceding claims,
c h a r a c t e r i z e d i n t h a t
a plurality of monitoring handling devices (CIH 11; 12) are
disposed in a public land mobile network (4).

30 9.[sic] The method according to one of the claims 1 to 8,
c h a r a c t e r i z e d i n t h a t
only one monitoring device (11; 12) is disposed in a public
land mobile network in each case.

11. A device (CIH 14), in particular for performing the method according to one of the preceding claims, having an interface to at least one switching device (border gateway 11, 12) for receiving data to be intercepted,
5 having a memory containing a list of addresses and keys of a plurality of listening stations (6; 7; 8; 9), having an interface for transmitting data to be intercepted from a terminal device (1), said data having been received
10 by a switching device (11) via the first interface, to an IP address of a listening station (6; 7; 8; 9), said address having been identified on the basis of the identity of the user (MSISDN, ISDN, MEI etc.) and the list stored in a memory in the device (14).

15